REMARKS

A telephone interview was held with Examiner Zee regarding the objection to claim 56 and the rejection of claim 56 under 35 USC 112. The courtesy extended by the Examiner is greatly appreciated.

Regarding the objection, the Examiner stated that he has no problem with entering an amendment that changes "for" to "configured to." To advance prosecution, the claim is so amended.

Regarding the rejection of claim 56 because, according to the Examiner, the phrases "long-term" and "short-term" render the claim in definite, the Examiner stated that he is not ready to commit to enter an amendment that changes "long-term policy" and "short-term policy" to "first policy" and "second policy," so this change in NOT introduced.

Applicant respectfully traverses the rejection. The terms "long-term" and "short-term" are labels of two policies, and they make the claim no more indefinite than if the phrases were "first policy" and "second policy." Put another way, there is nothing in the claims that can possibly raise the question "how long is long-term" and/or "how short is short term." Hence, the claim is not indefinite.

The claim was also rejected because the term "request" has an insufficient antecedent basis. Applicant respectfully traverses. The first time the term "request" appears is at line 5, where it a request (a) for the identification authority server to prepare an identification certificate, and (b) and to send it to the user computer. The "said request" that is referred to in the same clause (four lines later) is obviously referring to that request. A totally different request is defined at line 15. It is to provide both the previously prepared identification certificate and a validity statement, to the verification authority. The next clause focuses on the verification authority and specifies a module configured to verify "said request." Clearly the request being referred to is the only request that has any relevance to the verification authority; to wit, the request last mentioned in the claim, which is the request that provides the identification certificate and the validity statement to the verification authority. *No other interpretation is possible*. Therefore, it is respectfully submitted that no antecedence problem exists, and that claim 56 complies with 35 USC 112, second paragraph.

Claim 56 was rejected under 35 USC 103 as being unpatentable over Muftic, US Patent 5,745,574 in view of Van Oorschot et al, US Patent5,699,431. Applicant respectfully traverses.

The Muftic reference teaches a hierarchy of devices. With reference to FIG. 1 it may be observed that the highest (root) level is a PRA level, the next level (national) is the PCA level, and the third level (state) is the CPA level. Additional (lower) levels exist, and at each one of those levels there are (or may be) certification authorities (elements marks "CA"). With reference to the description at col. 5, lines 19-34, it is taught that the root level is the distinguished certification authority representing a root node of a certification hierarchy "or registration authority (RA) level" and that clearly corresponds to the aforementioned PRA level. It is also taught that the PCA level (second level) is the "policy certification authority." and that the policy certification authorities certify the certification authorities (CAs) at the third level. Those third level CAs can certify other CAs, presumably at the fourth and lower levels.

The Examiner asserts that Muftic discloses a "security policy server," an "identification authority server," a "revocation authority server," a "verification authority server" and a "user computer." Applicants respectfully disagree.

For the "identification authority server" the Examiner points to the *certificate authority*. There is no "certificate authority" in the reference. so it is assumed that the Examiner meant *certific*<u>*ation*</u> *authority*; i.e.. the clements marked CA in FIG. 1.

For the "security policy server" the Examiner point to the *policy certificate authority*. There is no "policy certificate authority" in the reference, so it is assumed that the Examiner meant *policy certific*<u>*ation*</u> *authority*; i.e., the elements marked PCA in FIG. 1.

The Examiner does not identify any element that constitutes the "revocation authority" but points to col. 13, lines 1-12 and, in particular, to the teaching of a revocation list. The paragraph that contains the pointed to text states:

> As discussed above, to validate a certificate reliably, the validator must ensure that none of the certificates utilized in validation has been revoked. To ensure that. the validator must have a correct certification revocation list from the common point of trust to the entity whose certificate is being validated. As shown in FIG. 6, a certificate revocation list is a data structure which contains a signature of the

> issuing party (600) together with algorithm ID and parameters used to sign the list, the electronic ID of the issuer (610), the last update date and time (620), the next scheduled update date and time (630) and a list of revoked certificates (640), arranged as shown. for example, in block 650. Revoked certificates are denoted by their sequence numbers in a sequential order and for each sequence number list the serial number of the certificate being revoked and the date and time of its revocation.

The Examiner asserts that the above-quoted paragraph teaches the module specified in claim 56; but applicant respectfully disagrees. Respectfully, what needs to be taught ins a specific module in a specific server. In applicant's view the reference does not have a revocation authority (which communicates with each of the other authorities via the public network) and does not have the claimed module.

The claim specifies a module that stores a memory validity statement – in the singular – in response to a policy that is NOT the policy that is used to create the identification certificate, and that validity statement includes a verification status at some temporal reference. The Examiner, however, points to an entire list, and that list is not **a validity** statement that is stored in response to a particular policy (short-term policy). Rather, it appears to be a list of certificates, where the list is augmented with entries, as needed; and the entire list of certificates is updated in unison. Hence, it is respectfully submitted that there is no module in the Muftic reference that properly corresponds to the module specified in the second clause (following the preamble) of claim 56.

The third clause of claim 56 specifies a means that, basically, receives a request from a computer to the effect "please send my identification certificate (that is found in the "identification authority") and my validity statement (that is found in the "revocation authority") to a verification authority. All three authorities are distinct – in the sense that they communicate with each other via a public network. The Examiner has not identified what the Examiner considers to be the "verification authority" and, respectfully, applicant believes that the reference has no "verification authority." The Examiner points to teachings in col. 7, lines 1-20, but that text teaches only the notion that to ensure validity of a certificate it is necessary to consult with all of the revocation lists (which are found in different certification authorities) and to consult with the certification authority that issued the certification. The passage does not teach providing, in response to a request by the user computer to have ITS OWN identification certificate AND its corresponding validity statement. The Examiner also points to teachings in col. 13, lines 42-52. Respectfully, those teachings also do not teach providing, in response to a request by the user computer to have ITS OWN identification certificate AND it corresponding validity statement. Therefore, it is respectfully submitted that the third clause of claim 56 is not taught by the Muftic reference.

As for the last clause of claim 56, the Examiner effectively admits that this module is not taught by the Muftic reference, but asserts that the Van Oorschot et al reference does disclose such a module and that it would have been obvious for one of ordinary skill in the art to modify the Muftic invention with the additional feature of Van Oorschot et al. Applicants respectfully disagree. First, because the Muftic reference's structure is such that the solution employed by the Muftic reference suffices, and there is no need to employ, or benefit to be garnered from employing, the teachings of Van Oorschot et al. Second, even if a person skilled in the art were to undertake to create a module as taught by Van Oorschot et al, it would still not be a module in a verification authority server that is distinct from all of the other servers (communicating with those servers through the public network). Third, the Van Oorschot et al reference does not provide that which is missing from the Muftic reference, as demonstrated above relative the other modules. Accordingly, it is respectfully submitted that claim 56 is not obvious in view of the combination of the Muftic and Van Oorschot et al references.

In light of the above amendments and remarks, applicant respectfully submits that all of the Examiner's objections and rejections have been overcome. Reconsideration and allowance are respectfully solicited.

Respectfully,
Stuart Gerald Stubblebine

Dated: 7/17/08

By Henry Brendzel
Henry T. Brendzel
Reg. No. 26,844
Phone (973) 467-2025
Fax (973) 467-6589
email brendzel@comcast.net